AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, [redacted], being duly sworn, depose and state the following:

AGENT BACKGROUND

1. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed in this capacity since June of 2015. I have been a member of sworn law enforcement since September of 2001. [redacted] I am currently assigned to the FBI Tampa field office in Tampa, Florida. In my capacity as a Special Agent, I have conducted a variety of national security and criminal investigations. I have investigated many different federal crimes including those involving national security, computer intrusions, intellectual property rights violations, mail and wire fraud, drugs, and violent crimes. Many of the crimes that I have investigated involved the use of email and social media to help perpetrate or further the crime. I have also assisted in the execution of numerous search warrants, including on electronic accounts, resulting in the seizure of paper, electronic, and other forms of evidence.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant for a residence located at [redacted] Tampa, FL 33604 (Target

Location). The Target Location includes an unattached secondary suite, which is located on the curtilage of the property.

3. There is probable cause to believe that the Target Location, as described in Attachment A, contains the fruits, instrumentalities, and/or evidence of:

a. an intentional unauthorized access of a computer, in violation of 18 U.S.C. § 1030; and

b. an intentional interception and disclosure of wire, oral, or electronic communication, in violation of 18 U.S.C. § 2511.

Said violations of federal law are collectively referred to in this affidavit as the "Target Offenses." Consequently, there is probable cause to search the Target Location for evidence of the Target Offenses.

4. Because this affidavit is provided for the limited purpose of establishing probable cause for the search warrant, I have not included all aspects of the investigation. Rather, this affidavit is intended to show merely that there is probable cause for the requested warrant. I am familiar with the following facts based upon my personal involvement in the investigation, as well as information I have obtained from other law-enforcement agencies and regulatory bodies and open source information, including news reports and reports from civilian cybersecurity-research firms.

BACKGROUND ON TWITTER

5. Twitter owns and operates a social networking and microblogging service of the same name that can be accessed at http://www.twitter.com and via

the Twitter mobile application ("app"). Generally, Twitter allows users to register and create an account; to personalize (if desired) an account profile page; and to send and receive communications via the platform. These functionalities are discussed in more detail below.

6. Twitter permits its users to communicate via messages that can contain photos, videos, links, and/or a maximum of 280 characters of text. Users can choose to share these messages, called "Tweets," with the public or, alternatively, to "protect" their Tweets by making them viewable by only a preapproved list of "followers." Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Users can also Tweet a copy of other Tweets ("retweet") or Tweet a reply to another Tweet. Users can also indicate that they like a Tweet by clicking on a heart icon that appears next to each Tweet on the platform.

7. While individuals are not required to register with Twitter to view the content of unprotected Tweets, individuals must register for a Twitter account to send Tweets, to "follow" accounts in order to view protected Tweets, and to send and receive direct messages. A user may register for an account for free by visiting Twitter's website or via the Twitter app. When a user creates a new Twitter account, Twitter assigns that account a unique User ID ("UID"). A user must also select a password as well as a unique Twitter username (also known as a "handle"). Twitter then appends the @ symbol in front of whatever username the user selects to create the Twitter username. The user may also select a different name (the "display name"), which is not automatically preceded by the @ symbol, to be displayed on his

profile picture and at the top of his Tweets alongside his Twitter username. The display name can include symbols similar to emojis. The user can change the user's password, username, and/or display name at any time, but the UID for the account will remain constant.

8. At the time of account creation, Twitter asks the user for certain identity and contact information, including: (1) name; (2) email address and/or telephone number; and (3) month and year of birth. Twitter also keeps certain information relating to the creation of each Twitter account, including: (1) the date and time at which the user's account was created; and (2) the method of account creation (e.g., website or Twitter app).

9. Upon the creation of a Twitter account, a generic profile page is automatically created for the user. This page displays information, including: (1) the user's Twitter username; (2) the display name; (3) the number of Twitter accounts the user is following; (4) the number of Twitter accounts that are following the user; and (5) Tweets sent by the user (although, as noted above, if the user has chosen to protect their Tweets they will be visible only to preapproved "followers"). The user can personalize this page by posting a personal picture or image (known as an "avatar") to appear on the page and/or a banner image to appear across the top of the profile page. The user can also add text to create a short biography, to identify the user's location, to provide a link to the user's website, or to specify the user's date of birth.

10. As noted above, Twitter users can use their respective accounts to send and receive communications. If a Tweet includes a Twitter username that is preceded by the @ symbol, that is referred to as a "mention." The Twitter user mentioned in the Tweet will receive a notification informing the user that the user has been mentioned and showing the content of that Tweet. Similarly, if another Twitter user replies to a Tweet sent by a user, the user who sent the original Tweet will receive a notification that someone replied to that message, and the notification will show the content of that reply.

11. A registered Twitter user can also "like" a Tweet by clicking a heart icon on a Tweet sent by another user. If another user "likes" a Tweet that is posted by the Twitter user, a notification will appear in the user's account identifying what Tweet was liked and who liked it.

12. Twitter users can also opt to Tweet with their location attached. This functionality is turned off by default, so Twitter users must opt-in to utilize it. However, if a Twitter user enables Twitter to access the user's precise location information, the Twitter user will have the option of attaching the user's location (e.g., the name of a city or neighborhood) to a Tweet at the time it is sent. If the user uses Twitter's in-app camera to attach a photo or video to the Tweet while the functionality is enabled, the Tweet will include both the location label (e.g., the name of a city or neighborhood) of the user's choice as well as the device's precise location in the form of latitude-longitude coordinates. The user can turn this functionality off

(thereby removing the user's location from Tweets) at any time, and the user can delete the user's past location data from Tweets that have already been sent.

13. A Twitter user may choose to "follow" another Twitter user. If a Twitter account is unprotected (i.e., privacy settings have not been enabled), the user can follow another user simply by clicking the "follow" button on the other user's Twitter profile page. If a Twitter account is protected (i.e., privacy settings have been enabled), the user can follow another user by clicking the "follow" button and waiting for the other user to approve the request. Once an account is followed by a Twitter user, the Tweets posted by the account the user follows will appear in the user's Twitter Home timeline. Every time a Twitter user follows another account, Twitter sends a notification to the account being followed to inform that account holder about the new follower. Each user's Twitter profile page includes a list of the people who are following that user and a list of people whom that user follows. Twitter users can "unfollow" other users whom they previously followed at any time. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting based on the types of accounts that the user is already following and who those people follow.

14. Twitter collects and retains information about a user's use of the Twitter service, to include: (1) content of and metadata relating to Tweets and Direct Messages; (2) photos, images, and videos that are shared via Twitter and stored in the user's Media Timeline; (3) the identity of the accounts that a user follows and the accounts that follow the user's account; (4) the content uploaded to a user's profile

page, including the user's avatar, banner image, and bio; (5) information about Tweets the account has liked; (6) information about Lists associated with the account; (7) information about the Spaces that a user has participated in, including the host of the Space, its start and end times, and information about other attendees; and (8) applications that are connected to the Twitter account. Twitter also collects and retains various other data about a user and the user's activity, including:

a. logs of Internet Protocol ("IP") addresses used to login to Twitter and the timestamp associated with such logins;

b. transactional records reflecting, for example, when a user changed the user's display name or email address;

c. the identities of accounts that are blocked or muted by the user; and

d. information relating to mobile devices and/or web browsers used to access the account, including a Twitter-generated identifier called a UUID that is unique to a given device.

15. Additionally, providers of electronic communications services and remote computing services often collect and retain user-agent information from their users. A user agent string identifies, among other information, the browser being used, its version number, and details about the computer system used, such as operating system and version. Using this information, the web server can provide content that is tailored to the computer user's browser and operating system.

16. In my training and experience, evidence of who was using a Twitter account and from where, and evidence related to criminal activity of the kind described above and below, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

17. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Twitter account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

18. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Twitter can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date, and time) may be evidence of who used or controlled the account at a relevant time. Similarly, device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators

to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

19. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

20. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

21. Therefore, Twitter's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Twitter. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

STATEMENT OF PROBABLE CAUSE

22. Law Firm #1,[1] legal representation for a broadcast network ("NetworkCo"), contacted the United States Attorney's Office for the Middle District of Florida and the FBI in early November 2022 to report an unlawful network intrusion incident, which had occurred on October 6, 2022.

23. On that date at approximately 4:30 p.m. EDT, a program host ("Host") for the NetworkCo's news arm, NetworkCo News, conducted an interview ("the interview") of a celebrity ("Celebrity") in Los Angeles. As the interview was being recorded, it was being streamed from the onsite location to New York City via satellite. Backup streams of the interview content were transmitted using encrypted and proprietary software over the internet to NetworkCo servers in New York City by another company ("StreamCo"), a video contribution technology company hired by NetworkCo to provide live video technology and related services. Portions of this interview were later broadcast by NetworkCo News during a television program(s) aired on October 6 and 7, 2022.

24. On October 11, 2022, a different media company's website ("WebPub"), published unauthorized excerpts from the interview conducted on October 6, 2022. The article from WebPub was entitled, "Watch the Disturbing

[1] The identities of potential victims, witnesses, and third parties have been anonymized in this affidavit to protect their privacy and the integrity of the federal criminal investigation.

[Celebrity] Interview Clips That [NetworkCo News Host] Didn't Put on Air." The article included six links[2] to interview excerpts on YouTube, which had been edited from the original content and never released by NetworkCo News to the public. Additionally, NetworkCo did not authorize release of any part(s) of the unaired interview.

25. As a result of this information leak, NetworkCo hired a digital forensics company ("DFCo") to investigate the incident. Through a digital forensic investigation, DFCo was able to determine that the interview had been intercepted by an unauthorized user during live transmission. The investigation by DFCo revealed the information contained below in paragraphs 26 through 30 of this affidavit.

26. Through open-source research, it was determined that StreamCo network user credentials and an associated password that had been designated to another broadcast network ("Network #2") were exposed on a radio-station website of a Network #2 radio affiliate located in Tennessee. Said credentials were exposed as early as January 16, 2022, and were found on the Internet Archive (The Way Back Machine).

---

[2] Articles and links are as follows: "Celebrity Vaccinated" at https://www.youtube.com/watch?v=qVbmgup1oG8, "Celebrity on Planned Parenthood" at https://www.youtube.com/watch?v=qn6PTWBXmpU, "Celebrity: 'We're no longer trauma drunk'" at https://www.youtube.com/watch?v=jqwOb-cPyLE, "Celebrity on Kwanzaa and Hannukah" at https://www.youtube.com/watch?v=soGtt2OU8ms, "Celebrity on Virgil" at https://www.youtube.com/watch?v=sWOicUe7Qsk, and "Celebrity on Energy Communities" at https://www.youtube.com/watch?v=0DgC8MJfC_8.

27. Through review of StreamCo network logs, it was determined that IP address 47.197. 207.14 (the IP address) was logged into the StreamCo network using the Network #2 credentials contemporaneously with the stream of the interview and for the entire duration. The IP address was first observed on StreamCo network logs on August 22, 2022, and repeatedly thereafter until at least October 14, 2022.

28. Using open-source tools, it was determined that the IP address resolved to Tampa, Florida, and more specifically the residence of Timothy Burke and his spouse, who reside within the confines of the Middle District of Florida. DFCo discovered four web domains being hosted from the IP address, which included one web domain associated with Burke's spouse and the following three associated with Burke:

- burke-communications[.]com: This website for Burke's media consulting company resolves to 47.197.207.14, according to commercial domain lookup repositories. This is an active domain that was created on June 3, 2019, and is registered through a proxy registrar called Wild West Domains.
- ilovecitr[.]us: Burke's professional website, which provides prior work samples and links to his social media accounts, resolves to 47.197.207.14, according to commercial domain lookup repositories. This is an active domain that was created on November 30, 2012, and is registered through a proxy registrar called Wild West Domains.

- mocksession[.]com: This website, which focuses on making memes regarding sports and music, is owned and operated by Burke and resolves to 47.197.207.14, according to commercial domain lookup repositories. It was created on November 25, 2005, and is registered through a proxy registrar called Wild West Domains.

29. Burke is the former Director of Video Editing for a popular news website. Burke also previously worked for at least two other media outlets as an investigative journalist. While not presently working in the media as a news journalist, Burke maintains a presence by collecting video clips and information and disseminating them via the internet. Currently, Burke owns and operates Burke Communications, which is advertised on its website as a media consultation company.

30. The research by DFCo further revealed that a violator using the IP address entered StreamCo's restricted computer network environment using the Network #2 credentials without authorization. Once there, the violator had access to StreamCo's system of URL-based video feeds and, with that knowledge, could determine the non-public URL and the StreamCo specific identifier for NetworkCo, which would then have allowed the violator to contemporaneously intercept the live electronic video feed, eavesdropping on the conversation between the NetworkCo News Host and Celebrity without authorization. Investigation to date leads your affiant to believe that the violator then recorded the interview and disseminated the contents of the electronic communication without authorization.

31. Open-source information provided by DFCo was later confirmed to be accurate by the FBI investigative team.

32. Further review of Burke's website burke-communications.com as of February 24, 2023, revealed several links to other related webpages. On a linked page titled "archives" Burke states, "Our archive of live news and sports programming reaches back to 1969, consumes more than 50 terabytes[3] of cloud storage space, and is fully indexed with metadata and closed captioning text whenever available." Additionally, on a page labeled "facts," Burke lists that he retains 181,000 gigabytes of video archive data.

33. Further review of Burke's website ilovecitr.us as of February 24, 2023, revealed a section labeled "HOW WE DO IT," which contains three subsections titled "HARDWARE," "SOFTWARE," and "ARCHIVING." The Hardware section states, "32 TV tuners monitor feeds from satellite, cable, fiber optic, and IPTV sources 24 hours a day using a mix of macOS and Linux-based machines." The Software sections states, "Proprietary Python[4] scripting combines with the industry-standard ffmpeg package across both platforms to maintain full HD quality and retain the original Dolby 5.1 audio streams. Finally, the "Archiving" section states, "Tens of thousands of raw broadcast footage in one of the largest private

[3] 50 terabytes of data is roughly equivalent to 50,000 gigabytes of data.

[4] Python is a computer programming language often used to build websites and software, automate tasks, and conduct data analysis. Python is a general-purpose language, meaning it can be used to create a variety of different programs and is not specialized for any specific problems.

archives of live news and sports video in the world, unedited and in its original broadcast format whenever possible."

Interview of StreamCo CTO and The StreamCo Network

33. On December 20, 2022, agents from FBI Tampa interviewed the Chief Technical Officer (CTO) for StreamCo. The CTO stated that he became aware of the unauthorized intrusion incident on October 13, 2022, when NetworkCo notified him of the leaked interview excerpts. NetworkCo requested that StreamCo provide all applicable network logs to assist in a forensic investigation. StreamCo provided all logs which were deemed by StreamCo to be relevant.

34. The CTO stated that the StreamCo network is a system that streams content from point to point on a non-public network. Clients who currently utilize the StreamCo network for streaming include many established, major media companies. The stream is sent from an origin, a transmission unit, on this occasion located in Los Angeles, CA, to a receiver at a different location, on this occasion located at NetworkCo Headquarters in New York City. Each unit has up to four channels, or "instances," each denoting a separate video camera. Each receiver is assigned a universal identifier unique to that receiver for use by StreamCo. The StreamCo network utilizes a Python script to generate this StreamCo identifier as digits in a Uniform Resource Locator (URL), ultimately used to access and identify streamed content. In the StreamCo network, content is streamed via HLS[5] streaming

[5] HLS Streaming, also referred to as HTTP Streaming, was released by Apple in 2009 and is currently the most widely used format for streaming video content over the internet.

and via a separate stream over satellite to ensure redundancy. Live streams are encrypted from point to point; however, the HLS live streams pass through the StreamCo server while in transit, where they are decrypted in low resolution making it viewable for the purpose of quality management. The signal is then encrypted again and continues to the receiver at the final location where it is recorded and stored in normal high-resolution format.

35. The CTO said that due to an error in the application programming interface (API) of the StreamCo network, it would have been possible to utilize developer tools embedded in the web browser to access a full list of StreamCo identifiers across the StreamCo network. If a user had a basic understanding of how the StreamCo identifiers were created by the Python Script, it would be possible for a user to link certain StreamCo identifiers to certain clients, allowing the individual to target and monitor streaming content over multiple StreamCo identifiers/clients. Once a user authenticated into the StreamCo network, due to another API error, that individual could potentially access any StreamCo identifiers, regardless to which client it belonged, without reentering user credentials. Additionally, if an individual knew both a StreamCo identifier and the format of the HSL stream query used by StreamCo (both of which were exposed by the aforementioned API errors), that individual would be able to create a URL to access any active StreamCo device through an HLS-compatible viewer without authenticating into the StreamCo network.

36. The CTO said that nobody by the name of Timothy Burke works at or has worked at StreamCo, nor did anyone by that name have authorization to access the StreamCo network or any content therein.

Interview of NetworkCo CTO

37. On November 30, 2022, agents from FBI Tampa interviewed the CTO for NetworkCo regarding the intrusion. The CTO stated that there were two unidentified IP addresses which accessed the live stream of the interview. One, an IPV6, was observed on the logs having accessed approximately the last 30 minutes of the interview. IP address 47.197.207.14 was the only unauthorized IP address which was logged on for the entirety of the interview stream.

38. The CTO stated that the interview streamed via satellite as its primary method. It also streamed via HLS through StreamCo. The satellite feed had multiple instances of loss of service or transmission. The leaked content had no signs of these instances of lost signal, and therefore must have derived from the HLS stream. NetworkCo conducted an internal investigation into the source of the leaked content and concluded that it was not possible that the content had been leaked by a NetworkCo employee.

39. According to the CTO, Timothy Burke was not currently, nor had he ever been, an employee of NetworkCo. Likewise, Burke did not have permission to access and release the leaked interview excerpts.

Interview of Network #2 BEMS

40. On January 10, 2023, agents from FBI Tampa interviewed the Broadcast Engineer Maintenance Supervisor (BEMS) for Network #2. The BEMS stated that the credentials, [Network #2-Network][6]-Demo, are used at Network #2 for demonstration purposes when reselling access to the StreamCo network to Network #2 affiliates, which is done via contract with StreamCo. These credentials are only authorized to be utilized by the Network #2 sales team.

41. The BEMS advised that Timothy Burke does not, nor has ever, worked for Network #2, nor did he have authorization to use the credentials to access the StreamCo network.

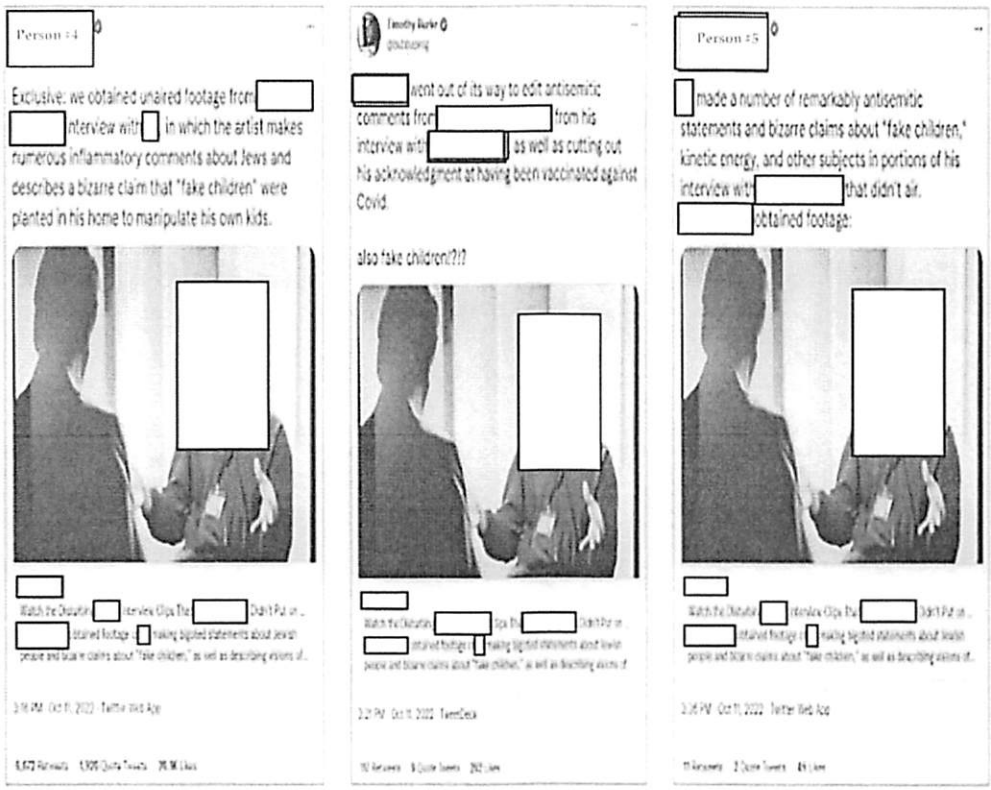
The Twitter Account

42. Investigators discovered relevant Twitter activity from Twitter account @b[redacted]g, which is linked to Timothy Burke via his website burke-communications.com.

43. Twitter subscriber records for @b[redacted]g reveal that the account was created on or about December 12, 2006, and is currently associated with email address t[redacted]ke@gmail.com. The account was logged into as recently as January 28, 2023, from IP address 47.197.207.14. The phone number associated with the account is a known telephone number associated with Burke.

[6] The term "Network #2-Network" is used pursuant to the effort throughout this affidavit to anonymize the identities of potential victims, witnesses, and third parties.

44. The investigation has revealed that on October 11, 2022, at 3:16 p.m. EDT, Person #4, a WebPub reporter, tweeted a link to the above-mentioned article—"Watch the Disturbing [Celebrity] Interview Clips That [NetworkCo News Host] Didn't Put on Air"—which was the first appearance of the unaired interview excerpts in the media. The Tweet contained a comment plus a still photo extracted from one of the unauthorized aired interview excerpts. ***Approximately 5 minutes later***, @b[redacted]og (Burke) tweeted the same still photo from the interview with a different comment. ***Approximately thirty seconds following Burke's Tweet***, Person #4 retweeted Burke's Tweet. Finally, ***on the same day approximately 15 minutes after Person #4's retweet***, a second WebPub representative, Person #5, tweeted the same still photo with different commentary. The interview photo in question was in low definition, with a reflection in the upper left corner of the screen. This leads investigators to believe that the image was likely captured using a secondary recording device as the image was shown on a computer screen. The relevant Tweets are shown below.

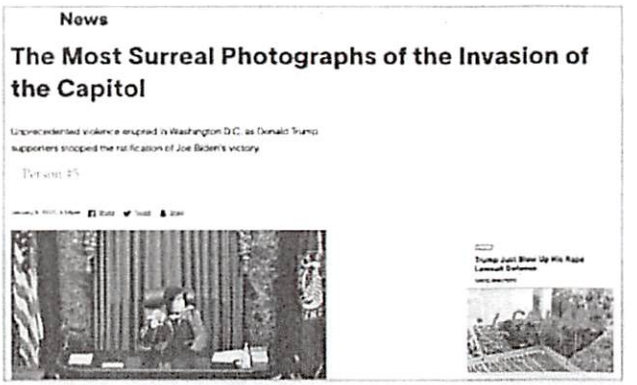


45. Review of LinkedIn profiles for Burke, Person #4, and Person #5 revealed that all three individuals were employed by a design, technology, and science website[7] from January of 2018 through July of 2018.

46. Moreover, the three individuals have continued to associate with one another following their overlapping time at the common employer, in that: (1) Burke "follows" Person #4 and Person #5 on Twitter; and (2) Burke, Person #4, and Person #5 have publicly conversed using Tweets and replies. As a pertinent example, Person #5 posted an article on January 6, 2021, which was originally posted to

[7] The referenced website launched in 2002 and merged with another website in 2015, after which it began to post articles on subjects such as science fiction, fantasy, futurism, science, technology, and astronomy.

Burke's Twitter page. Notably, Burke's post of the article occurred at 3:42 p.m. on that day, and Person #5's article was published 14 minutes later, at 3:56 p.m.



47. Burke has demonstrated his knowledge concerning video streaming technology by posting multiple Tweets using @b[redacted]og about different video feeds, resolution, aspect ratio, and other elements of videography, as well as specific information regarding the resolution and picture quality of NetworkCo streams. Burke has also posted multiple Tweets via @b[redacted]og about having experience with StreamCo's streaming, as well as having knowledge of NetworkCo's streaming methods. For example, Burke posted a Tweet on December 22, 2021, about seeing "…high quality [StreamCo] signals every day…[,]" despite Burke having never worked for StreamCo and never having been authorized to access the StreamCo network. The referenced Tweet is included below.

The Telephone Records

48. Review of domain burke-communications.com revealed Burke listed his telephone number as [redacted]. Using open-source tools, investigators determined that this number was serviced by T-Mobile.

49. Records from T-Mobile showed that, from October 10, 2022, through November 29, 2022, telephone number [redacted] had incoming or outgoing calls with telephone number XXX-XXX-3112 on at least 10 occasions. There were no contacts outside of these dates between the two numbers from January 1, 2022, through January 28, 2023.

50. Open-source research on telephone number XXX-XXX-3112 revealed it was associated with Person #5, an employee of WebPub. This telephone activity occurred contemporaneously with the release of the above discussed previously unaired video excerpts.

51. Investigators believe it possible that the above discussed secondary device utilized to record the unauthorized interview excerpts could have been a cellular telephone, and the recordings of those excerpts could remain on that device.

IP Address 47.197.207.14

52. IP address 47.197.207.14 resolved to Frontier Communications ("Frontier") using open-source tools. Records secured from Frontier during the ongoing investigation reveal that the subscriber of the IP address as of October 6, 2022, was Burke's spouse and that the subscriber's address was [redacted], Tampa, FL 33604.

53. A review of pertinent logs provided by StreamCo revealed that IP address 47.197.207.14 was viewing content of the interview on and off throughout the interview duration. Log activity showed that 47.197.207.14 was the only IP address which viewed all the aforementioned unlawfully intercepted and distributed excerpts in their entirety, making it highly likely that the individual using that IP address was the individual who distributed the excerpts to WebPub. Notwithstanding, a second IP address, [redacted], was observed in the logs as having viewed content on three occasions during the interview. However, only two of the unlawfully distributed excerpts were viewed by the user of that IP address, thereby confirming that the user or users at that address was/were not the person(s) who intercepted and distributed the six excerpts to WebPub.[8]

---

[8] Open-source tools have revealed to investigators that IP address [redacted] resolved to Comcast. Subscriber records obtained from Comcast further revealed that the account belonged to Person #2 at [redacted] Auburn, WA. Follow-up efforts support the belief that two individuals reside at that location, Person #2 and Person #3. Records checks by NetworkCo, StreamCo, and Network #2 all show that neither Person #2 nor Person #3 were or are employees of the companies; and therefore, neither person was or is authorized to access the StreamCo network using said companies'

54. As explained above, Burke states on his website that he retains 181,000 gigabytes of archived video, with 50,000 gigabytes being stored on the cloud. Investigators believe it is likely that the remaining video is stored at the Target Location. This belief is based upon various facts and evidence to include photographs posted to social media by Burke and statements made on his websites. Some photographs posted by Burke on Twitter show multiple computers and monitors clustered together in what appears to be an electronics center. Investigators also believe it likely that the script and hardware device(s) utilized to monitor and intercept the interview video content is stored at the Target Location.

55. A review of the Hillsborough County Property Appraiser's website showed that the secondary suite is constructed of wooden planks with drywall and central air. The secondary suite is visible from the roadway at the Target Location. The secondary suite is pink in color, like the residence, and has siding, windows, and a front entry door. In a drive-by of the rear of the secondary suite, an exterior air conditioner condensing unit was visible to the south side, and a second entry door was visible to the rear (west). The secondary suite appears to be finished living space suitable to house Burke's electronics equipment.

56. A review of the Florida business registry website at sunbiz.org revealed that a business named Mocksession, LLC is registered to Timothy J. Burke at the

---

passwords. The individual who accessed the StreamCo network from said IP address and the purpose for that access is currently unknown and remains under investigation.

Target Location, listing Burke as the registered agent. This, when taken with the above information, particularly that information contained in paragraphs 54 and 55, leads investigators to believe it likely that the Target Location is the location of Burke's electronic equipment and related storage.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

57. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Target Location, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

58. I submit that if a computer or storage medium is found on the Target Location, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation as explained above, I am aware that computer equipment was used to access, without authorization, one or more restricted computer network(s) and to unlawfully intercept live electronic video feeds and to distribute the same, in violation of 18 U.S.C. §§ 1030 and 2511. There is reason to believe that there is a computer system currently located at the Target Location.

59. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Target Location because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the

innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information

indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when, as in this investigation, an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

60. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of

storage media. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. As explained above, Burke lists that he retains 181,000 gigabytes of video archive data. 181,000 gigabytes equal approximately 181 TB (terabytes), or 181 million MB. Depending upon how the data is stored and the equipment available to transfer and image that data, the required imaging process could consume as much as 35 days.

c. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations.

Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

61. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

62. Because it is believed that at least one other person shares the Target Location as a residence, it is possible that the Target Location will contain storage media that are predominantly used, and perhaps owned, by one or more persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

63. As noted above, four web domains are believed to be hosted from the pertinent IP address, which includes one web domain associated with Burke's spouse and three domains associated with Burke. As a result, it is likely that Burke and/or his spouse are conducting some legitimate business for one or more companies (collectively, the "Companies") at the Target Location. The seizure of the Companies' computers may limit the Companies' ability to conduct legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If Burke, his spouse, or an employee associated with a Company so requests, the agents will, to the extent practicable, attempt to provide the requesting person(s) copies of data that may be necessary or important to the continuing function of a Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

64. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to

search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID

registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience and the criminal conduct described herein I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device

manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Target Location and

reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; or (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

65. Based on the affiant's training and experience, and the facts as set forth in this affidavit, the affiant respectfully submits that there is probable cause to believe that the Target Location contains the fruits, instrumentalities, and/or evidence of the Target Offenses. For those reasons, the affiant requests that the Court issue the proposed search warrant. The Government will execute the warrant by serving it on Burke at the Target Location.

REQUEST FOR SEALING

The affiant further requests that the Court order that all papers in support of the application, including the affidavit and search warrant, be sealed until further

order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal the documents because their premature disclosure may seriously jeopardize that investigation.

FURTHER AFFIANT SAYETH NAUGHT.

[redacted]

Special Agent [redacted]
Federal Bureau of Investigation

by telephone

Sworn to me this 4th day of May, 2023.

SEAN P. FLYNN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Description of Premises to Be Searched

The Target Location is known as [redacted] Tampa, FL 33604 and is identified as follows:

The Target Location is a one-story single-family home that is pink in color with a brown shingle roof and stucco exterior. The front of the Target Location faces east toward North Tampa Street and has several white and pink columns which support the covered porch and carport, located to the north side of the Target Location. A mailbox at the end of the driveway bears the number [redacted]. An unattached secondary suite exists on the property to the rear, or west, of the Target Location, facing east. This secondary suite is also colored pink, with siding, a white roof, and a teal front door.

The Target Location includes any vehicles, trailers, sheds, and other buildings on the curtilage of the property. The Target Location is located within the City of Tampa, which is in the Middle District of Florida.

ATTACHMENT B
Particular Things to be Seized

All records and other evidence relating to violations of 18 U.S.C. § 1030 (intentional unauthorized access of a computer), and 18 U.S.C. § 2511 (intentional interception and disclosure of wire, oral, or electronic communication) (collectively, the "Criminal Conduct"), those violations involving Timothy Burke and occurring after August 1, 2022, including:

1. Any books, records, or ledgers associated with items or services sold to or received from companies, or individuals associated with said companies, involved in posting or hosting electronic streaming content.
2. Hard copy and/or electronic records of contacts and exchanges (including drafts and final versions, and any related subparts) with companies, or individuals associated with said companies, involved in posting or hosting electronic streaming content.
3. Evidence reflecting payment in any form, including cash, checks, wire transfers, online payment service, ACH transfer, and/or cryptocurrency (to include hardware wallet(s) and pass phrase(s)) from companies, or individuals associated with said companies, involved in posting or hosting electronic streaming content.
4. Computers, storage media, cell phones, smart phones (including the smart phones associated with telephone number [redacted]), used as a means to

commit the Criminal Conduct described above, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

   d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

6. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; or (2) hold a device found at the premises in front of the face those same individuals and activate the facial

recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.